CR1-QKD
CR2-NEA

QUANTON® CR

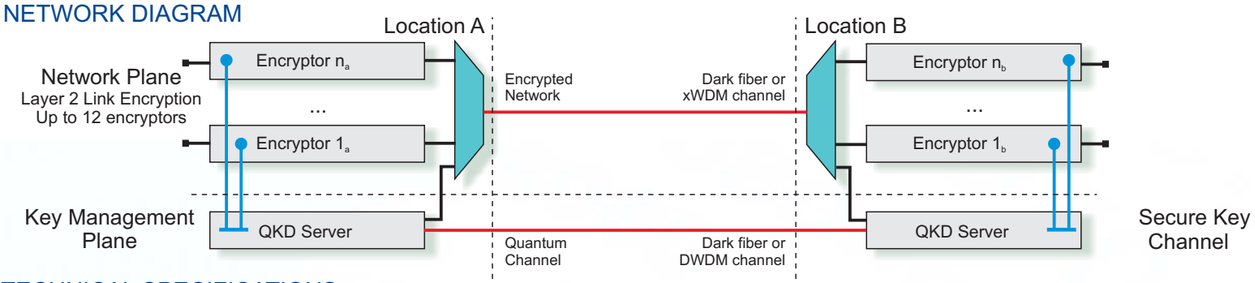
High Speed Data Encryption & Quantum Key Distribution

Long Range DWDM Optical Fiber
Convergent Network Connectivity
Integrated Network Management

pursue perfection

CR1-QKD

NETWORK DIAGRAM



TECHNICAL SPECIFICATIONS

CR2-NEA

leap! ahead

Quantum Key Distributor

- Quanton® Key Distribution Appliance provides secure quantum key distribution with key management functionalities. Combined with the Quanton® Encryption Appliances, it is a scalable and highly secure solution. Quanton® Key Distribution Appliance provides secure quantum keys for up to 12 high performance Quanton® Encryption Appliances, protecting data during transmission outside the secure perimeter of the company without impacting network performance. Maximum standard transmission distance is 100 km (longer distance is available upon request).

Quantum Safe Security

- Quantum Key Distribution uses the intrinsic laws of quantum physics to secure the exchange of the encryption keys between different encryptors. The quantum principle that measurement introduces perturbation is used to ensure that there is no eavesdropping or interception attempt on the key exchange. In addition the use of quantum keys ensures forward secrecy of all communications. The Quanton® Key Distribution Appliance can be added to optical fiber data center links to ensure long-term data protection by providing quantum keys to Quanton® Encryption Appliances.

Back-Door Proofed

- The exchange of secret encryption keys, which the encryption security is based upon is performed by a dedicated appliance: the Quanton® Key Distribution Appliance. A fundamental principle of quantum physics - observation causes perturbation - is exploited to exchange secret keys between two remote parties over an optical fiber with unprecedented security. The Quanton® Key Distribution Appliance autonomously produces, manages and distributes secret keys to up to twelve encryption appliances.

Incredible Speed

- The Quanton® Key Distribution Appliance works in conjunction with Quanton® Encryption Appliances for high-speed encryption based on the proven Advanced Encryption Standard (AES). Point-to-point wire-speed encryption with minimum latency and no packet expansion is made possible by operating at the layer 2 of the OSI model. Standard network protocols up to a bandwidth of 10Gbps are supported. These encryptors have received stringent security accreditation (Common Criteria EAL4+ and FIPS 140-2). In order to guarantee the highest level of security, a dual key agreement process is used. Separate encryption keys are exchanged using Quanton® Key Distribution and conventional techniques before being combined to produce a resulting key, as strong as the strongest of the two keys.

Secure MultiLink Encryptor

- Quanton® Encryption Appliances ensure the protection of data in transit, offering the ultimate combination of high network performance with quantum-safe security. The Quanton® Encryption Appliance platform encrypts Ethernet and Fibre Channel traffic up to an aggregated throughput of 100Gbps on local and storage area networks for data back-up and recovery, as well as on fully meshed global WAN networks for international operations.

European Solution

- The latest Quanton® Encryption Appliances use a key material generated by IDQ's Swiss-certified quantum TRNG (True Random Number Generator) to ensure highly secure, truly random keys. Such quantum cryptography is provably secure, ensures anti-eavesdropping detection and provides long-term forward secrecy against brute force hacking and attacks by quantum computers. Additional security is provided by advanced anti-tamper proofing and physical protections, as well as best-practice separation of duties.

Comprehensive Integrity

- Encryption with ultra-low latency and no packet expansion or packet loss (so called "bump in the wire"). Quanton® Encryption Appliance devices use state-of-the-art AES 256 bit encryption, with the optional GCM mode providing data integrity on a per-packet level as well as confidentiality. The transport security feature masks the data flows on the network to ensure that traffic patterns do not reveal critical information.

Network Connectivity

- Ethernet and Fibre Channel protocols are supported. The devices have (or are pending) Common Criteria and FIPS security accreditations. Quanton® Encryption Appliances are agnostic to network-equipment and integrate seamlessly into existing network infrastructures. The simple installation procedure, smart network discovery and set-and-forget operation ensures rapid deployment and minimal ongoing maintenance requirements.

Management and Monitoring

- CypherManager allows the easy implementation and monitoring of enterprisewide security policies for audit and compliance. Simple provisioning and scalable management are enabled, either locally or remotely via secure connections (inband or out-of-band). CypherManager acts as the Certificate Authority by signing and distributing X.509 certificates to the encryptors, as well as accepting third party certificates. It is compatible with SNMPv3 compliant network management tools (eg NetView, OpenView, Tivoli).

TECHNICAL SPECIFICATIONS

Quanton® Quantum Key Appliance

Ethernet Encryption	• point-point,1-10 Gbps per card
Fibre Channel Encryption	• point-point 1/2/4 Gbps per card (8 Gbps under development)
Other Protocols	• SONET/SDH (3, 12, 48, 192), ATM (3, 12)

Network Performance

Throughput	• 100% bandwith available
Latency	• less than 15 µs

Encryption

Algorithms	• AES 256-bit • CFB mode (up to 1Gbps) • CTR mode (up to 10Gbps)

Security

Security Accreditation	• Common Criteria EAL4+ • FIPS 140-2

Key Management

Management	• Seamless and automated key management
Dual key agreement	• conventional and quantum cryptopgraphy
Key refresh rate	• 1 key/minute up to 12 encryptors
Quantum Key Distribution	• BB84 and SARG, up to 50km (100km upon request)
Conventional key agreement	• RSA-2048, master key

Local and Network Interfaces

Quanton® QK Appliance	• SC optical connector, WDM compatible
Quanton® Encryption Appliance	• SFP transceivers (up to 5 Gbps), XFP transceivers (10Gbps)

Random Number Generator

Quanton® QK Appliance	• Quantis Quantum Random Number Gen.
Quanton® Encryption Appliance	• Hardware Random Number Generator

Access Control

Identification	• Role-based identification for separation of duties

Audit Trail

Logs, Alarms, Changes	• Event log, audit log, date and time of secure connection • Configuration changes • Interface Status • Alarms

Secure Management

Quanton® QK Appliance	• SNMPv3, Ethernet 10/100 Rj45, touch panel
Quanton® Encryption Appliance	• SNMPv1, v2 and v3, Ethernet 10/100 RJ45, browser TLS or IPSec trusted path In-band on local and network interfaces

Indicators

Quanton® QK Appliance	• Touch panel, 240x180 pixels
Quanton® Encryption Appliance	• Two line 20 characters LCD display, LED indicating status of local interface, network interface, temperature, battery status, system operation and secure status, power

Environmental

Formfactor	• 4U rackmount black
Weight	• ~16kg (dependent on configuration)
Power Supply	• 350W fully redundant
AC Input	• 100 - 240V, 50-60Hz
Operating Environment	• max 40°C 0 - 80% RH (non-condensing) at 40° C

Quanton® Encryption Appliance

Ethernet Encryption	• point-point, hub & spoke, fully meshed 1-10 Gbps per card
Fibre Channel Encryption	• point-point 1/2/4/8 Gbps per card (16 Gbps under development)
Maximum Throughput	• 100 Gbps
General Features	• Protocol and Application Transparency • Encrypts Unicast, Multicast and Broadcast traffic • Automatic network discovery and connection, resilience to network outages
Network Interfaces	• SFP+, SFP

Security and Encryption

Security	• Tamper resistance and anti probing barriers • Policy based on MAC address or VLAN ID • IDQ Quantum Random Generator • Support for Quantum Key Distribution • Automatic seamless key management
Encryption	• AES-GCM mode for integrity • AES 128 or 256 bit keys • CTR, GCM, CFB for FC as Encryption modes

Performance

Overhead	• Low overhead full duplex line rate encryption
Latency (per encryptor)	• Less than 8ms via Ethernet Less than 1ms via Fibre Channel

Management

Convergent Connectivity	• Flexible policy engine with secure local and remote provisioning and management (SNMP v3) • In-field firmware upgrades • SNMPv1/2 monitoring (read only) • Support for external (X.509v3) Cas • CRL and OCSP (certificate) server support

Physical Dimensions and Maintenance

Formfactor	• 4U rackmount black
Physical Dimensions	• 436x460x175mm
Weight	• ~22kg (dependent on configuration)
Power Supply	• 300W fully redundant
AC Input	• 100 - 240V, 50-60Hz
Operating Environment	• max 40°C 0 - 80% RH (non-condensing) at 40° C

www.novarion.com • Email: office@novarion.com • Phone: +43 1 5441159-0

Powered by IDQ FROM VISION TO TECHNOLOGY